Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A method of speeding up packet filtering used in a network security apparatus, comprising:

generating a first hash space according to at least one rule used to filter the packets received by the network security apparatus, and the first hash space presenting a mask characteristic value set;

generating a second hash space according to at least one of the packets received by the network security apparatus, ~~and~~ wherein the second hash space ~~with~~ has the same size as the first hash space, presenting a packet characteristic value set;

performing a specific Boolean operation ~~with~~ for the first hash space and the second hash space; and

~~determining whether the packet characteristic value set is out of the mask characteristic value set, according to the results of said Boolean operation, then it is decided whether the packet is allowed~~ allowing the packet to pass through the network security apparatus according to the results of said Boolean operation.

Claim 2 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 1 wherein the network security apparatus comprises a firewall so that the rule can be pre-installed in the firewall.

Claim 3 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 2 wherein the firewall comprises a search filter assisting the rule of the firewall to filter the packets.

Claim 4 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 1 wherein the content of each rule comprises at least a specific mask that needs to be filtered.

Claim 5 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 4 further comprising:

converting the specific mask in each rule into binary codes;

converting each relative address of any code with bit ~~values~~ value "1" in the binary codes into a corresponding address pointing to the first hash space in order to obtain a set of the corresponding ~~addresses, with regard to~~ addresses of each said specific mask, pointing to the first hash space; and

collecting each set of the corresponding addresses pointing to the first hash space together thereby presenting ~~a mask~~ the characteristic value set ~~with regard to all of said specific~~ of all intended filtered masks in the first hash space.

Claim 6 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 5 further comprising:

utilizing the relative address of any code with bit ~~values~~ value "1" in the binary codes ~~to be~~ as a key of at least a specific hash function, and then performing the hash operation to obtain each corresponding address pointing to the first hash space.

Claim 7 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 5 further comprising:

respectfully generating a first hash ~~space, with regard to each specific mask,~~ space having a specific mask characteristic value, according to each set of the corresponding addresses pointing to the first hash space; and

totaling each bit value with the same address in each said first hash space having specific mask characteristic value thereby presenting a mask characteristic

value set ~~with regard to~~ all of the ~~specific~~ intended filtered masks in ~~one~~ the first hash space.

Claim 8 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 1 wherein each packet comprises at least an IP address that ~~needs~~ intends to be checked.

Claim 9 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 8 further comprising:

converting ~~at least one~~ the specific IP address ~~in~~ of each said packet into binary codes;

converting each relative address of any code with bit value "1" in the binary codes into a corresponding address pointing to the second hash space thereby obtaining a set of corresponding addresses, ~~with regard to~~ of each said IP address, pointing to the second hash space; and

collecting each set of the corresponding addresses pointing to the second hash space together thereby presenting a packet characteristic value set with regard to the ~~at least one~~ packet in the second hash space.

Claim 10 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 9 further comprising:

utilizing each said relative address of any code with bit value "1" in the binary codes ~~to be~~ as a key value of at least a specific hash function, and then performing a hash operation ~~thereby obtaining~~ to obtain each corresponding address pointing to the second hash space.

Claim 11 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 9 further comprising:

respectively generating the second hash ~~space, with regard to each said IP address,~~ space having a specific IP address characteristic value, according to

each set of the corresponding addresses pointing to the second hash space; and

totaling each bit value with the same address in each said second hash space having specific IP address characteristic value thereby presenting a packet characteristic value set ~~with regard to~~ of the at least one packet in ~~one~~ said second hash space.

Claim 12 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 1 further comprising:

when at least one ~~of~~ bit ~~values~~ value of the results of the Boolean operation in each the first hash space and the second hash space is out of value "0", ~~it is ensured that~~ and the packet characteristic value set is out of the mask characteristic value set ~~and therefore~~ , then the packet can be allowed to pass through the network security apparatus.

Claim 13 (currently amended): A method of speeding up packet filtering used in a network security apparatus, including ~~a method~~ procedures of generating a mask characteristic value set ~~with regard to~~ of all specific masks that ~~need~~ intend to be filtered, comprising the steps of:

extracting each of the specific masks from at least one predefined rule ~~pre-installed~~ in the network security apparatus;

converting each of the intended filtered specific masks into corresponding binary codes;

for each of the specific masks, searching the corresponding binary codes for a set of M relative addresses, where M equals to the quantity of bits with a bit value of "1" in the corresponding binary codes and each relative address uniquely equals to a bit number where the bit value is "1" in the corresponding binary codes;

for each of the specific masks, converting each relative address ~~with bit value "1" in the binary codes~~ into a corresponding address pointing to a hash space

thereby obtaining a set of the corresponding addresses, with respect to each specific mask, pointing to the hash space; and

collecting all the ~~each~~ set of the corresponding addresses pointing to the hash space together thereby presenting a [[I]] mask characteristic value set ~~with regard to~~ of all of the specific masks in the hash space.

Claim 14 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 13 further comprising:

utilizing each said relative address of any code with bit value "1" in the binary codes ~~to be~~ as a key of at least a specific hash function, and then performing a hash operation to obtain said corresponding address pointing to the hash space.

Claim 15 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 13 further comprising:

for each specific mask, respectively generating a hash ~~space, with regard to each specific mask,~~ space having a specific mask characteristic value, according to each set of the corresponding addresses pointing to the hash space; and

totaling each bit value with the same address in each said hash space having specific mask characteristic value thereby presenting ~~a mask~~ the characteristic value ~~set with regard to all of the specific masks in one~~ sets of the intended filtered masks of said hash space.

Claim 16 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 13 further comprising:

setting the bit values of all ~~sets of~~ the corresponding addresses pointing to the hash space to be "1" thereby presenting a mask characteristic value set with regard to all of the ~~specific~~ intended filtered masks in the hash space.

Claim 17 (currently amended): A method of speeding up packet filtering used in a

network security apparatus, ~~including a method,~~ a procedure of generating a packet characteristic value set with regard to specific IP address, ~~addresses that needs to be checked~~, comprising:

extracting each specific IP address intends to be checked from at least one packet received from the network security apparatus;

converting the each specific IP address in each packet into corresponding binary codes;

for each of the specific IP addresses, searching the corresponding binary codes for a set of M relative addresses, wherein M equals to the quantity of bits with a bit value of "1" in the corresponding binary codes and each relative address uniquely equals to a bit number wherein the bit value is "1" in the corresponding binary codes;

for each of the specific IP addresses, converting each relative address ~~with bit value "1" in the binary codes~~ into a corresponding address pointing to a hash space in order to obtain a set of the corresponding addresses, with regard to each of the specific IP addresses, pointing the hash space; and

collecting all sets of the corresponding addresses pointing to the hash space together thereby presenting a ~~packet~~ characteristic value set of the IP address with regard to the packet in the hash space.

Claim 18 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 17 further comprising:

utilizing each relative address of any code with bit value "1" in the binary codes ~~to be~~ as a key of at least a specific hash function, and then performing a hash operation to obtain the corresponding address pointing to the hash space.

Claim 19 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 17 further comprising:

respectively generating a hash space~~, with regard to each of the specific IP~~

~~address,~~ having a specific IP address characteristic value, according to each set of the corresponding addresses pointing to the hash space; and

totaling each bit value with the same address in each said hash space having a specific IP address characteristic value thereby presenting a packet characteristic value set ~~with regard to~~ of the ~~at least one~~ packet in the hash space.

Claim 20 (currently amended): The method of speeding up packet filtering ~~in~~ of claim 17 further comprising:

setting the bit values of all sets of the corresponding addresses pointing to the hash space to "1" in order to present the packet characteristic value set.